|  |  |  |  |
| --- | --- | --- | --- |
|  |  | SIEM Group Assignment (Core)  Otis Smith / Cybersecurity Professional / 8.29.23 |  |
|  |  |  |  |
| Pipette dropping liquid in a petri dish | | | |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | |
|  |  | TABLE OF CONTENTS |  |
|  |  | Summary …………………………..  Discovery……………………………  Vulnerability……………………….  Exploitation………………………..  References.………………………..  Mitigation………………………….. |  |



|  |  |  |
| --- | --- | --- |
| Summary |  | |
| This report outlines the process of Digital Evidence Collection, focusing on creating an image of an OS using SystemBack and verifying data integrity with Autopsy. The objective is to ensure the validity of evidence in a digital forensics investigation. The report covers the steps from downloading SystemBack to comparing MD5 hashes in Autopsy, demonstrating a thorough and successful evidence collection process.  A hand holding a glowing city  Description automatically generated | |  |
| Discovery  The discovery phase involved downloading the SystemBack file from a provided link, navigating through the terminal to unzip and install SystemBack, and configuring its settings for live system creation. Key steps included selecting the appropriate operating system (Ubuntu 20.04), creating a new live system named "KaliImage," and patiently waiting for the image creation to complete. | |  |
|  | |  |

|  |  |  |
| --- | --- | --- |
| Vulnerability |  | |
| One potential vulnerability mentioned is the limitation on filesystem size. If the filesystem becomes too large, it may hinder the creation of a correct image. Users are advised to manage file sizes or consider a fresh installation of the Kali instance. | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Exploitation |  | |  | |  |
| No exploitation activities were conducted in this process. The focus was on creating a valid image of the operating system for forensic analysis. | |  | |  | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  | | --- | --- | --- | --- | | References |  |  |  |  1. Downloading SystemBack:    * Link: <https://drive.google.com/file/d/1ytht-uPrk8feoNnLq3IpCygWchVU0Hcr/view> 2. Commands:    * Unzipping SystemBack: tar -xvf systemback-install\_pack-1.9.4.tar.gz    * Installation: sudo ./install.sh    * Checking hash: md5sum filename 3. Autopsy:    * Autopsy command: sudo autopsy |  | |
|  | |  |

|  |  |  |
| --- | --- | --- |
|  |  | |
|  | |  |

Mitigation:

1. **Enhance User Management:**
   * Strengthen password policies and regularly review user access.
2. **Limit Sudo Access:**
   * Carefully assign sudo privileges and monitor sudo logs.
3. **SSH Security:**
   * Implement secure SSH configurations, including key-based authentication.
4. **Firewall Rules:**
   * Review and adjust firewall rules to limit unnecessary network exposure.
5. **Regular Security Audits:**
   * Conduct routine security audits, addressing identified vulnerabilities promptly.
6. **Educate Users:**
   * Provide comprehensive security training to users.
7. **Continuous Monitoring:**
   * Establish continuous monitoring mechanisms for real-time threat detection.
8. **Access Control for SIEM:**
   * Implement strict access controls within the SIEM system.
9. **Documentation and Training:**
   * Maintain thorough documentation for system configurations and security measures.
10. **Backup and Recovery:**
    * Implement regular backup procedures for critical components.
11. **Incident Response Plan:**
    * Develop and regularly update an incident response plan.
12. **Regular Software Updates:**
    * Keep all software, including Elastic SIEM and Kali Linux, up to date.

In conclusion, the assignment provided a comprehensive understanding of Elastic SIEM, web log analysis, and Kali Linux integration. Identified vulnerabilities were addressed through a combination of user management, access controls, and continuous monitoring. The experience emphasized the crucial role of a SIEM system in enhancing overall cybersecurity.